EXHIBIT N

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC., Plaintiff, vs. KEYSIGHT TECHNOLOGIES, INC., and IXIA, Defendants.	)	Case No. 2:17-cv-383-HCM-LRL

DECLARATION OF DR. ERIC COLE IN SUPPORT OF PLAINTIFF CENTRIPETAL NETWORKS, INC.'S OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

I, Eric Cole, declare:

1. I was retained as an expert witness by Centripetal Networks, Inc. ("Centripetal") to provide expert analysis and opinions. I am willing to testify in this action regarding the opinions set forth in this declaration.

I. EXPERIENCE AND QUALIFICATIONS

A. Curriculum Vitae

2. I hold a master's degree in computer science and a doctorate in information security and have worked in the cyber and technical information security industry for over 25 years. During this time, I have actively been involved with the design and development of a wide range of software products. I am fully aware of both the process of developing software and also the importance and criticality of keeping software up to date and current based on changing market conditions.

3. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

4. The details of my education are summarized in my curriculum vitae ("CV") attached hereto as Exhibit 1 of this Report.

5. I am the founder of Secure Anchor Consulting where I provide cyber security consulting services and lead research and development initiatives to advance information systems security. I am a Fellow and instructor with The SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world.

6. I am an author of several security courses such as SEC401-Security Essentials and SEC501-Enterprise Defender.

7. In addition, I have also been the curriculum lead for cyber defense for SANS which involves overseeing the management and creation of new courses in addition to all of the existing courses.

8. I have worked for the government for 8 years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have held various top-secret security clearances with Department of Defense (DOD), CIA, and Nuclear Regulatory Commission (NRC). I have worked for a wide range of government organizations including FBI, National Security Agency, CIA, Department of Energy, DOD, the Treasury, Secret Service and the NRC.

9. While serving as a Senior Officer for the Central Intelligence Agency as Program Manager / Technical Director for the Internet Program Team with Office of Technical Services, I implemented the Internet Program Team that designs, develops, tests, and deploys internet security products in 3 to 6 month intervals. In this role, I received a letter of appreciation from the DCI (Director Central Intelligence) and six Exceptional Performance Awards.

10. As a member of the Information Security Assessment Team with the Office of Security, I also evaluated and performed security assessment of network operating systems to identify potential vulnerabilities and solutions. I also designed a large scale auditing system with automated review capability and worked on several virus investigations for the Office of Security.

11. In my role as Chief Information Officer for the American Institutes for Research, I have repaired and developed IT infrastructures for various organizations and provided technical support for the Defense Advanced Research Projects Agency (DARPA), an

agency of the United States Department of Defense responsible for the development of new technologies for use by the military.

12. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as technical advisor in high-profile security projects for government clients including the Department of Defense, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

13. As Chief Technical Officer for McAfee, I executed the technology strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. I was not only responsible for the development of new products, but also the ongoing challenge of keeping existing products up to date and relevant in the market. In this capacity I worked closely with groups tasked with the development of intellectual property.

II. SUMMARY OF OPINIONS

14. My opinions, expressed herein, are based on my knowledge and experience in the field of computer science and with respect to standard industry practice in the field of computer science and network security. This includes the development and maintenance of software to be implemented in various products.

15. In my industry experience in the development of software both at Lockheed Martin and McAfee, in addition to my work advising startups on the marketable and key

feature set of new products, I am very familiar with software, especially software development in the context of computer security products. In the current highly competitive market, security products must be constantly updated to meet customer demands. In my experience, a product that is not update frequently quickly becomes obsolete in the market. In addition, many companies do not change the name of the products, but the feature set is completely different. For example, a company might be selling a product that has the same name for the last 5 years, but the technology, functionality, and feature set is completely different. Therefore, it is customary to completely re-write a product but keep the name of the product the same.

16. It is not only regular practice but it is customary for new technologies to be implemented into older products. This is particularly true in the field of network security where technology is constantly evolving in order to protect against threats, which are developed and released on a daily basis from all over the world. As the years have gone by, threats are becoming more and more prevalent. For example, Symantec provides a timeline of major events in Internet Security, which indicates that the first PC virus was created in 1985, and by 1993, "[t]raffic on the Internet expand[ed] at an annual growth rate of 341,634 percent." Ex. 2 at 2 (Symantec Timeline); *see also* Ex. 3 (GCN Timeline); Ex. 4 (NATO timeline). Since then, threats have continued to increase at a rapid rate. McAfee recently issued a threat report in December 2017 describing the increase in threat statistics stating that "[t]he biggest number of the quarter is [Symantec's] count of new malware, which reached an all-time high of 57.6 million new samples, an increase of 10% from Q2." Ex. 5 at 2 (McAfee Labs Threat Report). The AV-TEST Institute, an Independent IT-Security Institute, indicated that it

"registers over 250,000 new malicious programs every day." Ex. 6 (Malware Statistics & Trends Report).

17. Given the constant development of new malware, a security company's products would be severely outdated and would not be able to protect against these newly developing threats without continuously making changes to software to combat malware. These changes to software may come in the form of software updates, which are done in order to address software vulnerabilities. Ex. 7 at 1 (Norton – The Importance of general software updates and patches) ("A software vulnerability is usually a security hole or weakness found in an operating system or software program. Hackers exploit this weakness by writing code to target a specific vulnerability, which is packaged into malware."); *see also* Ex. 8 (McAfee – Why Software Updates are So Important) ("skipping software updates "is a mistake that keeps the door open for hackers to access your private information, putting you at risk for identity theft, loss of money, credit, and more."). In other words, while a product may keep the same name, new technologies may still be implemented into the older products, to help prevent virtual attacks, for example.

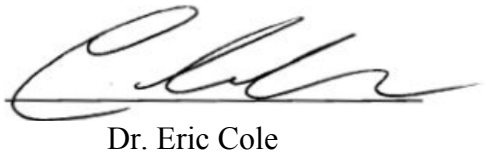
18. Based on my industry experience, it is not uncommon for software companies to develop source code for a product family using one similar codebase, and enable certain technologies and/or features in some, but not all of the products within that family, despite the ability of each of these products to fully support these technologies and/or features. While a technology or feature may be introduced into a code repository, a software company may decide to stagger the manner in which it decides to activate the technology or feature in its products. This decision can be based on both technical and business reasons. In my experience, it is not uncommon for less than 50% of the active code base to actually be

implemented or operational in a given product. This allows code to be modified or updated very quickly across many products without major re-work by the developers.

19. For instance, a software company may decide to not activate a technology or feature in one product, but allow its activation in others, due to time constraints of having to perform quality assurance on the product. Testing the product may require several months and/or years of observation in order to determine when the technology or feature operates in a satisfactory manner within the product. A company may decide to release one product with a certain feature to the market first, and then decide to enable this feature afterwards in the other products once the first product is released. During this testing period, consumers may be already aware of the technology or feature due to its implementation in other products.

20. A software company may also decide to not activate a technology or feature in a particular product because it may want to see how consumers react to it as implemented in a set of different products. Based on this consumer reaction, the software company may decide that it may not be worth investing time and resources to activate the technology or feature for its entire product line due to lack of consumer demand for the technology or feature.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on June 7, 2018, in Ashburn, Virginia.



Dr. Eric Cole

Dated: June 7, 2018

Respectfully submitted,

/s/ Stephen E. Noona

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com

Paul J. Andre (*pro hac vice*)
Hannah Y. Lee (*pro hac vice*)
James R. Hannah (*pro hac vice*)
Lisa Kobialka (*pro hac vice*)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
hlee@kramerlevin.com
jhannah@kramerlevin.com
lkobialka@kramerlevin.com

Christina L. Martinez (*pro hac vice*)
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Telephone: (212) 715-9000
Facsimile: (212) 715-8000
cmartinez@kramerlevin.com

Attorneys for Plaintiff,
Centripetal Networks, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on June 7, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will automatically send notification of electronic filing to:

William R. Poynter
Virginia State Bar No. 48672
KALEO LEGAL
4456 Corporation Lane, Suite 135
Virginia Beach, VA 23462
Telephone: (757) 238-6383
Facsimile: (757) 304-6175
wpoynter@kaleolegal.com

Christine M. Morgan (*pro hac vice*)
James A. Daire (*pro hac vice*)
John P. Bovich (*pro hac vice*)
Jonah D. Mitchell (*pro hac vice*)
Doyle B. Johnson (*pro hac vice*)
Christopher J. Pulido (*pro hac vice*)
REED SMITH LLP
101 Second Street, Suite 1800
San Francisco, CA 94105
Telephone: (415) 543-8700
Facsimile: (415) 891-8269
cmorgan@reedsmith.com
jdaire@reedsmith.com
jbovich@reedsmith.com
jmitchell@reedsmith.com
dbjohnson@reedsmith.com
cpulido@reedsmith.com

Attorneys for Defendants
Keysight Technologies, Inc. and Ixia

/s/ Stephen E. Noona

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3239
Facsimile: (888) 360-9092
senoona@kaufcan.com